73-G : __ __ __

Policy Enforcement for Enterprise System Integration and Interoperability

Lifeng Wang, Zhengping Wu
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Introduction

When policy-based management has been introduced in cross-domain organization collaborations and system integrations, we have to face to a trouble which is the policies of a domain cannot directly have match enforcement mechanism in its partner domain, due to most different systems from different domains or organizations have different high-level policy descriptions and low-level enforcement mechanisms. We have to manually update their enforcement mechanisms for system integration and interoperability. In this paper we propose a middleware architecture which is used to solve this problem. This middleware provides various functions to enforce policies across domains automatically or semi-automatically, such as gathering of policies in every participant domain and creating policy models for every domain. Once there is a new participant domain involved, its policy can be collected and integrated to the policy model. Finally, every specific policy rules following these models can be mapped to multiple enforcement mechanisms of participant domains. Once there is a policy has no matched enforcement mechanism in participant's domain, the policy can be reported to domain administrator for further deployment.

Middleware Architecture

Our middleware have a total of three layers architecture, which are high-level policy languages layer, intermediate level processing and translation layer and low level enforcement mechanism layer. Those three layer have two structures as illustrated in figure 1, the first structure can be explain as the left-hand side scenario which is a policy from domain A needs to be enforced in domain B. this situation happens when a new collaboration is established without any additional policy invoked, the policies of domain A are enforced directly by the enforcement mechanism of its partner B. The second structure an be described as the right-hand side scenario which is that a policy needs to be enforced over these two domains. It happens when a new collaboration is established with new policies invoked. Those new policies are obeyed by both domain and enforced by their enforcement mechanisms.

As we know, ontology is a formal representation of a set of concepts within a domain and the relationships between concept elements. So all the models used in this paper are described by OWL.

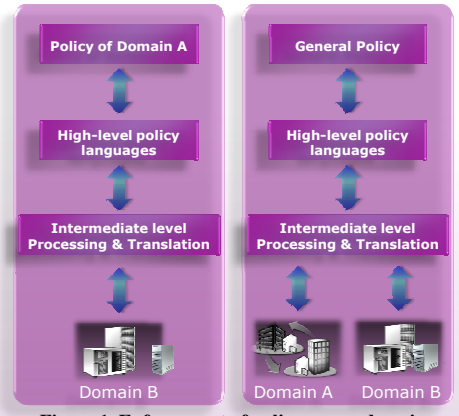

Figure 1 Enforcement of policy across domain boundaries

Case Study

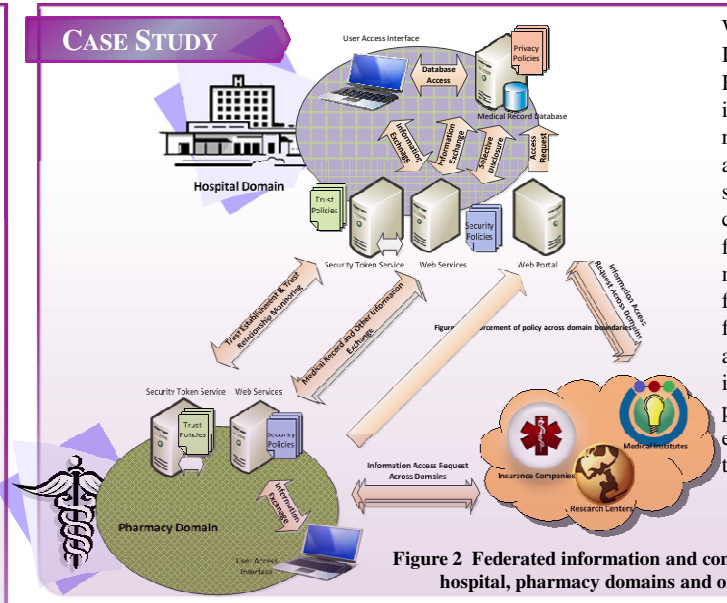

Figure 2 Federated information and control flows between hospital, pharmacy domains and other domains

We use the general enforcement architecture for a healthcare environment as case study. In the healthcare environment, system administrators need to define policies following HIPAA and other regulations for all electronic medical records and other digitized information; doctors and medical specialists can define security policies for medical records; and patients can define their own security policies and access control policies to authorize utilization or disclosure of their own information. As illustrated in Figure 2, system interactions between the hospital domain and the pharmacy domain, and different components within one domain are through web services. Security policies for security flows are described in WS-Security Policy, which are used for security protections of medical records and access control of other patient information. Trust policies for trust flows are described by WS-Trust for cross-domain federation activities. Privacy policies for privacy flows are described in WS-Policy format for privacy protections within and across domains. These policies need to be enforced in local domain as well as in domains involved in interactions. Our policy enforcement architecture can help to introduce policies to all the enforcement mechanisms of participant domains. Then, their policy enforcement for system integration and interoperability are generated automatically though our middleware.

Conclusion

When a number of enterprise domains participate in a collaboration, their collaboration and cooperation activities will be under the control of their mutual agreement and policies from other participants. It is hard to introduce a new set of policy enforcement mechanisms in local systems or applications, especially for dynamic policies and temporary federations. This paper proposes an enforcement middleware for policy federation to help map and translate dynamic and foreign policies. Following the case studies, the advantages of this enhanced new enforcement architecture are confirmed and can be summarized into three merits: administrators and users can choose their high-level policy languages with the most expressive capability; a domain's enforce mechanism is transparent to all of its partner; system integration and interoperability for policy management can be done automatically or semi-automatically.